REMARKS

Claims 1-45 remain pending in the Application. Claims 1-45 stand rejected by the Examiner. Claim 11 has been amended herein. Applicant traverses the rejections of claims 1-45.

Claim Rejections

Claims 1, 2, 4-8, 16-23, 31-40 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Vanstone et al. U.S. Patent No. 6,122,736 (hereinafter the "Vanstone reference"). Claim 3 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Vanstone, and further in view of applicant's own prior art admission. Claims 11-15, 26-30, 41-45 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Vanstone and further in view of the Heer reference (U.S. Patent No. 6,028,933). Applicant traverses these rejections.

Claim 1 recites that a plaintext message is encrypted into a ciphertext message and in the encrypting step, an ephemeral key pair is produced. That ephemeral key pair is then used in signing a digital signature. The Examiner maintains that the Vanstone reference discloses the encryption of the plaintext message into a ciphertext message wherein the encrypting step includes the step of producing an ephemeral key pair; and discloses signing a digital signature using the ephemeral key pair.

Applicant respectfully disagrees with the Examiner's position. Cryptography usually involves two distinct stages: key establishment and encryption/decryption. The Vanstone reference acknowledges the two distinct stages:

> Key establishment is the process by which two (or more) parties establish a shared secret key, called the session key. The session key is subsequently used to achieve some cryptographic goal, such as privacy. (Vanstone , col. 1, ll. 27-30).

In other words, in the first stage, called key establishment, two or more parties (in this context, computer systems) exchange information to establish a shared key, called a session key.

Then, once the session key is established, it is subsequently used in the second stage (e.g., called encryption/decryption). In the encryption/decryption stage, the sending party converts a message from what is known as "plaintext" to "ciphertext" by applying a mathematical transformation, which may be reversed only with the session key.

The two stages are independent. In some cryptographic approaches, the first stage may not even involve an automatic key establishment, and thus, keys may be exchanged manually, for example over the phone, and then manually entered in the computer systems. Furthermore, once keys have been exchanged, by any method, the information does not have to be encrypted. Also, some information may be encrypted and some may not.

The Vanstone reference is directed to the first stage in that the Vanstone reference discloses a method of overcoming deficiencies of previously known key establishment methods. The title of the Vanstone reference shows the sharp focus on the first stage: "Key agreement and transport protocol with implicit signatures." The Vanstone reference discloses stage 1 methods of exchanging the keys for providing better security (e.g., the Vanstone reference "...provide[s] a method of authenticating a pair of correspondents A, B to permit exchange of information therebetween..." (col. 2, ll. 64-65)). The "exchange of information" is not part of the first stage methods mentioned in the Vanstone reference. Rather the methods disclosed in the Vanstone reference are performed to enable a later secure exchange of information. Although the Vanstone reference may disclose methods using digital signatures, Vanstone is only using the digital signatures as a part of a stage 1 key establishment process. Accordingly, the Vanstone reference does not disclose the use of digital signatures in the encryption stage (e.g., when plaintext is encrypted).

Claim 1 of the present application recites a public key encryption process and system comprising the steps of: (a) encrypting a plaintext message into a cyphertext message, the encrypting step includes the step of producing an ephemeral key pair; (b) signing a digital signature using the

ephemeral key pair. The method is directed to a stage 2 (e.g., later stage) encryption process. At this second stage, the plaintext message is being encrypted, and consequently, element (b), signing a digital signature, is a part of the encryption method. Both instances of using a digital signature cited by Examiner, in the present office action dated 07/15/2004 (col. 3, ll. 3-12) and the office action dated 11/13/2003 (col. 5, ll. 6-8) disclose using digital signatures in the stage 1 key establishment process. This is evident because the cited sections are not referring to digital signatures in the context of encrypting a plaintext message (which is a later stage operation).

Accordingly, claim 1 as well as all claims dependent thereon, are patentable over the Vanstone reference.

To further clarify the multiple stage context, claim 11 has been amended to recite that at least a two stage public-key encryption process is used, wherein the first stage includes key establishment and the second stage includes encryption/decryption. Claim 11 further recites that the steps (a) and (b) of claim 1 are performed during the second stage (e.g., subsequent stage) of encryption. Because the Vanstone reference does not disclose steps (a) and (b) being performed during the second stage as required by claim 11, claim 11 is allowable for this additional reason.

The other independent claims (e.g., claims 16 and 31), in combination with their respective limitations, are directed to stage 2 processing and thus are allowable over the Vanstone reference. Because each of the pending independent claims are allowable, their respective dependent claims are also allowable.

Applicant also disagrees with other positions presented by the Examiner. For example, applicant disagrees with the position provided on page 2 of the office action wherein reference is made to applicant's own specification for an admission of prior art (e.g., applicant's specification, page 8, lines 5-17). The cited specification section in the office action is not applicable to the Vanstone reference since the hashing mentioned on applicant's page 8, lines 5-17 refers to hashing

that occurs in a different stage than to what the Vanstone reference is directed. In fact, this citation further illustrates the difference between the Vanstone reference and the instant claim in that the hashing (which the office action is referring to in applicant's specification) occurs in a stage different than a key establishment stage. This is further supported pictorially in applicant's Figure 2 which is the figure corresponding to applicant's text on page 8. Applicant's Figure 2 shows that lines 5-17 of page 8 (in reference to the hashing of the plaintext message) occurs in a later stage 70 and not during an earlier stage, such as a key establishment stage.

CONCLUSION

For the foregoing reasons, Applicant respectfully submits that claims 1-45 are allowable. Therefore, the Examiner is respectfully requested to enter this responsive amendment and to pass this case to issuance.

Respectfully submitted,

Date: Sept. 15, 2004

By: _____

John V. Biernacki
Reg. No. 40,511
JONES DAY
North Point
901 Lakeside Avenue
Cleveland, Ohio 44114
(216) 586-3939